~~SECRET~~

CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION

J-3
DISTRIBUTION: A, B, C, J, S

CJCSI 3210.01A
6 November 1998

JOINT INFORMATION OPERATIONS POLICY (U)

References: See Enclosure C.

1. (U) Purpose. This instruction provides joint policy and guidance for information operations (IO) in accordance with reference a.

2. (U) Cancellation. CJCSI 3210.01, 2 January 1996, is cancelled."

3. (U) Applicability. This instruction applies to the Joint Staff, Services, combatant commands, Defense agencies, and joint and combined activitles.

4. (U) Policy. See Enclosure A.

5. (U) Definitions. See Glossary.

6. (U) Responsibilities. See Enclosure B.

7. (U) Summary of Changes. This revision:

a. (U) The title and content of document are focused on ID in accordance with reference a.

b. (U) IO examples within policy enclosure have been updated.

c. (U) Addition of responsibilities for Joint Warfare Analysis Center, Joint COMSEC Monitoring Activity, Joint Spectrum Center, and Joint Task Force for Computer Network Defense (JTF-CND).

Classified By: Brig Gen Bruce A. Wright, J-39
Reason: 1.5(g)
Declassify On: X-4

~~SECRET~~

8. (U) Releasability. This instruction/manual/notice is not approved for electronic release on the World Wide Web (WWW); electronic release is restricted to the Joint Staff LAN only. Approval from the Office of Primary Responsibility (OPR) is required for further release of this instruction/manual/notice in electronic format on the WWW.

9. (U) Effective Date. This instruction is effective upon receipt.

10. (U) Security Instructions. This basic instruction is UNCLASSIFIED. Enclosures are classified as marked. Specific classification guidance and disclosure policy concerning IO-related issues are addressed in reference b.

For the Chairman of the Joint Chiefs of Staff:

DENNIS C. BLAIR
Vice Admiral, U.S. Navy
Director, Joint Staff

Enclosures:
A -- Policy
B -- Responsibilities
C -- References
Glossary

DISTRIBUTION

Distribution A, B, C, and J plus the following:

	Copies
Secretary of Defense	20
Chairman of the Joint Chiefs of Staff	2
Director of Central Intelligence	20
President, National Defense University	10
Director, Joint Command and Control Warfare Center	10
Commander, Joint Warfighting Center	10
Director, Information Operations Technology Center	10
President, Armed Forces Staff College	20

(INTENTIONALLY BLANK)

TABLE OF CONTENTS

(INTENTIONALLY BLANK)

ENCLOSURE A

POLICY

1. (U) Background

a. (U) IO focus on the vulnerabilities and opportunities presented by the world's increasing dependence on information and information systems (information systems include human operators, decision makers and human interaction within processes). OOO IO target and protect information, information transfer links, information gathering and processing nodes, and human decision making interaction with information systems. The ultimate target of offensive IO is the decision maker and the decision-making process (human or machine) in order to influence, deny, degrade, disrupt, destroy, or deceive the target resulting in desired outcome. At the tactical through strategic levels, the target of IO is the information-dependent process, whether human or automated. At the tactical level, IO would have as their objective the facilitation of friendly, or the disruption of adversary, combat operations, either short or long term. At the operational level, IO would have as their objective assisting in the achievement of campaign or operational objectives, or supporting tactical or strategic IO. At the strategic level, the IO objective is to assist in the achievement of a strategic national and theater objective. IO require complete integration so that the objectives and means at all levels is mutually supportive. Reference a outlines OOD IO policy.

b. (U) IO is one of many aspects of the US military's instruments of national power. OOD IO supports the overall US Government (USG) strategic engagement policy during peacetime, crisis, conflict, and post-conflict. The effectiveness of deterrence, power projection, and other strategic concepts greatly affects the ability of the USG to influence the perceptions and decision making of others. In peace and in times of crisis, IO help deter adversaries or potential adversaries from initiating actions detrimental to the interests of the USG or its allies, or to the conduct of friendly military operations. If carefully conceived, coordinated, and executed, IO will make an important contribution to defusing crises; reducing the period of confrontation; and enhancing the impact of diplomatic, economic, and military efforts; and can enable our ability to introduce military actions into the crisis area if necessary.

Classified By: Brig Gen Bruce A. Wright, J-39
Reason: 1.5(g)
Declassify On: X-4

c. (U) Even potential adversaries that lack advanced technology and capabilities to exploit information and information systems can conduct IO through use of physical attack, deception, propaganda, computer network attack (CNA), and other means. Some potential adversaries are developing advanced capabilities to exploit information and information system technologies. Examples include telecommunications, automated data processing, sophisticated decision aids, remote sensors, and other related systems. The spectrum of applied technologies range from established radio frequency, microwave, satellite, coaxial, and fiber optic transmission systems to new generations of digital and advanced personal communications systems. The ready availability and relatively low cost of these information technologies in world markets increases the likelihood that potential adversaries will employ them in advanced command and control systems, as components of advanced weapons systems, in other information systems, and as offensive capabilities. National-level infrastructures, including economic, industrial, and transportation systems that support national and military objectives, are also becoming increasingly dependent on automated control (e.g. Supervisory Control and Data Acquisition (SCADA)) and information systems for their operation. This growing acquisition and application of information technologies by potential adversaries presents friendly forces with new opportunities to achieve military objectives via the information realm.

2. (U) General. IO is full spectrum strategies, which have applications that may be used during peacetime and across the range of military operations at every level of warfare. IO must be synchronized with air, land, sea, space, and special operations -- as well as interagency and multinational operations -- in harmony with diplomatic, economic, and efforts to attain national and multinational objectives. The conduct of defensive IO is continuous, in both peacetime and conflict, and the capabilities and activities employed in IO are inherent parts of successful force protection. Offensive and defensive IO are mutually supporting and require the integration of various activities and capabilities. Examples of capabilities and activities include deception and counterdeception, electronic warfare (electronic attack and electronic protect), information assurance (IA), operations security (OPSEC), physical destruction, physical security, psychological operations (PSYOP) and counter-propaganda; computer network attack (CNA) and computer network defense (CND), counterintelligence, and potentially others. Although it is necessary that all aspects of IO related information dissemination be coordinated and synchronized, commanders must carefully manage the separation of PA and PSYOP functions to preserve the integrity and credibility of PA

operations. References c, h-j, m-o, and v-y provide guidance and principles for employment of individual activities and capabilities. IO may involve complex legal and policy issues requiring careful review. The following paragraphs illustrate employment of IO in differing scenarios.

a. (U) Military Operations Other Than War (MOOTW). IO may be employed to shape the global and regional environments to deter a crisis, control crisis escalation, or promote and maintain peace. The employment of offensive capabilities in these circumstances may require National Command Authorities (NCA) approval with support, coordination, deconfliction, cooperation, and/or participation by other USG Departments and agencies.

b. (U) Conflict. IO may be employed during MOOTW involving the use, or threatened use, of force or during wartime. IO can be waged inside and outside the traditional military battlefield at all levels of war. Specific capabilities applied during crisis or conflict, referred to as information warfare (IW), should be integrated. IO to achieve other than traditional military objectives may require Presidential approval.

c. (U) The following paragraphs illustrate employment of IO in differing theoretical scenarios. The OOO may be a supporting USG agency in certain scenarios. Future examples include, but are not limited to:

(1) (U) Peace Enforcement Operations

(a) (U) Objective: Implement peace accords between warring factions.

(b)(1)

(c) (U) PSYOP messages must be coordinated with PA, OPSEC, and other activities to ensure consistency and common purpose.

(2) (U) Counterdrug Operations

(a) (U) Objective: Reduce traffic and support of drug cartel operations.

(b)(1)

(3) (U) Counterproliferation of Weapons of Mass Destruction (WMD)

(a) (U) Objective: Disrupt adversary's WMD program.

(b)(1)

(4) (U) Deterrence

(a) (U) Objective: Deter invasion of country by regional aggressor.

(b)(1)

(5) (U) Disruption of Enemy Command and Control (C2)

(a) (U) Objective: Neutralize adversary command authority's ability to direct military operations.

(b)(1)

(6) (U) Influencing Adversary Groups or Individuals

(a) (U) Objective: Lower morale and combat efficiency of adversary soldiers.

(b)(1)

(c) (U) New technology may allow direct access to individuals, bypassing higher command and control structures, greatly reducing the adversary's strength of force.

(7) (U) Protect Friendly Information and Information Systems

(a) (U) Objective: Protect critical friendly information and information systems during operations.

(b)(1)

include the use of friendly offensive capabilities (CNA, physical destruction, and EW) to destroy or degrade adversary offensive IO.

3. (U) Guidance. The following is the Chairman of the Joint Chiefs of Staff's specific policy guidance.

(b)(1)

b. (U) Defensive Operations

(1) (U) IO will be employed to protect and defend information and information systems (processes used in C2, communications, weapon systems, etc.) used by US military forces relative to their value and risks associated with their compromise, degradation or loss of access. Defense of information through information assurance (IA) and other capabilities and activities is critical to the military's ability to conduct operations and is the responsibility of the combatant commanders, Services, and DOD supporting agencies. Various activities and capabilities range from technical security measures (traditional INFOSEC, hardening of communications sites, electronic warfare reprogramming, etc.) to procedural (OPSEC, counterintelligence, physical security, counter-propaganda, etc.) and must be integrated to defend information and defend information systems. Information assurance capabilities will be incorporated into information systems and employed continuously. Other defensive capabilities will be employed in accordance with existing policy, the assessed threat, and operational requirements.

(2) (U) The defensive information operations process includes measures taken to protect information systems, detect attacks or intrusions, restore capabilities lost or degraded by attacks or intrusions, and any response(s) to attacks or intrusions. The response process will determine motives and actors; establish causality, sponsorship, complicity, possible indications or warning of an attack, assessment of damage and may involve appropriate action against perpetrators. The restoral process will ensure the information system or information-based process is restored to its minimum required capability in the least amount of time. Joint Pub 3-13, "Joint Doctrine for Information

Operations," will provide additional guidance on the defensive IO process as does reference q.

c. (U) Information operations conditions (INFOCONs). INFOCONs similar to THREATCONs will be developed to heighten the defensive posture, defend against information attacks and mitigate damage that may result. Although INFOCONs are focused on information systems, an assessment of current situation and operations should be undertaken to see if other measures or changes in defensive posture should be taken to protect forces and operations. This may include assessment of OPSEC, physical security, communications security (COMSEC), THREATCONS, and other defensive active or passive measures. This assessment should also determine if the attacks against information systems are part of a larger IO (propaganda, diplomatic, terrorism, deception, and other activitles) to achieve adversary objectives.

d. (U) Intelligence

(1) (U) DOD capabilities, both offensive and defensive, rely heavily on intelligence. In many cases, the level of intelligence detail required for effective offensive and defensive IO is unprecedented. Working in support of the joint warfighter, the capability provider will identify the unique intelligence requirements -- both technical and nontechnical in nature -- needed to employ offensive capabilities against adversary vulnerabilities and assess adversary IO (intentions and capabilities) in support of defensive IO. IO intelligence requirements for targets and capabilities in support of operational plans must be articulated with sufficient specificity to the appropriate intelligence production center. The intelligence requirements will afford the Intelligence Community the opportunity to develop and refine the required priorities to provide adequate intelligence support.

(b)(1)

(b)(1)

f. (U) Training and Education. Joint and Service school curriculums will ensure that personnel are educated in the concepts of IO and appreciate the vulnerabilities inherent in their information systems and the opportunities that may be found in adversary systems. Combatant commands and Services will Integrate IO into exercises to enhance overall joint operational readiness.

g. (U) Joint Operations Plans. The combatant commanders will incorporate IO with deliberate (Operations Plans, Operations Plans Concept Format, and Functional Plans) and crisis action plans (operations orders and campaign plans) to accomplish their Unified Command Plan (UCP) assigned missions. Consideration and incorporation of IO concepts throughout the planning process will ensure that IO are applied across the spectrum of military operations at every level of joint warfare.

h. (U) Legal. IO conducted throughout the range of military operations may Involve complex legal issues. The complexities introduced by domestic, foreign, and international law make it critical that at the appropriate level of command legal counsel is involved in policy development as well as the development and employment of various techniques and capabilities. Military technologies, tactics, techniques, and procedures for conducting IO must undergo a legal review in accordance with reference e to ensure that they are consistent with the domestic and international legal obligations of the United States.

(INTENTIONALLY BLANK)

ENCLOSURE B

RESPONSIBILITIES (U)

1. (U) The following responsibilities are associated with implementing joint IO policy:

2. (U) The Chairman of the Joint Chiefs of Staff, as the principal military advisor to the President, the Secretary of Defense, and National Security Council, is responsible for developing and providing US military policy, positions, and strategy that support DOD IO operational planning as a part of the interagency process. To assist the Chairman, the designated Joint Staff directorate head will ensure the following:

a. (U) The Director for Intelligence (J-2) will:

(1) (U) Coordinate development of joint doctrine, strategy, and policy for intelligence support to IO within the Joint Staff and combatant commands.

(2) (U) Provide precise and timely intelligence for IO target development, selection, and post strike analysis to the combatant commands and Joint Staff.

(3) (U) Ensure combatant commands and/or the Joint Staff receive direct intelligence support to assist planning and execution of IO across the full range of military operations.

(4) (U) Work closely with the Joint Staff and combatant commands to coordinate the development of effective indications and warning methods to identify potential IO threats.

(5) (U) Assist in identifying friendly vulnerabilities and the most probable friendly targets within the threat capabilities and concept of operations.

(6) (U) Coordinate all intelligence support for the Joint Staff Information Operations Response Cell (JSIORC).

Classified By: Brig Gen Bruce A. Wright, J-39
Reason: 1.5(g)
Declassify On: X-4

b. (U) The Director for Operations (J-3) will:

(1) (U) Provide focal point for IO at Joint Staff. Collaborate with the Director, J-2; Director for Strategic Plans and Policy (J-5); Director for Command, Control, Communications, and Computer Systems (J-6); Director for Operational Plans and Interoperability (J-7); and the Director for Force Structure, Resources, and Assessment (J-8) to provide oversight of all joint IO matters. Joint IO matters include policy and strategy development, validation of capability requirements and programs, the IO Joint Warfighting Capabilities Assessment (JWCA) process, budget reviews and assessments, technology development, and security.

(2) (U) Ensure activities and capabilities are fully integrated into deliberate and crisis planning in a manner consistent with DOD IO policy.

(3) (U) Represent the Chairman of the Joint Chiefs of Staff and combatant commands in functionally oriented, National Security Council (NSC)-led interagency working groups (IWGs) concerning all IO matters.

(4) (U) Direct activation of the JSIDRC, which will be the focal point of all IO pertaining to CND and CNA within the Joint Staff.

(b)(1)

(6) (U) Coordinate with the Services, combatant commands, Defense agencies, and Joint Staff to develop joint IO doctrine.

(7) (U) Coordinate with the Director, J-7, and the Director, J-5, on joint IO training, education, exercises, and exercise evaluation; and on incorporation of IO into the operations plans and planning processes.

(8) (U) Coordinate with Services, combatant commands, combat support agencies (CSAs), and Joint Staff to optimize capabilities, minimize duplication, and de-conflict incompatibilities in current and future systems employed in IO.

c. (U) The Director, J-5, will:

(1) (U) Ensure employed activities and capabilities are fully integrated into deliberate and crisis planning, and joint exercises in a manner consistent with OOO ID Policy.

(2) (U) Coordinate with the Director, J-2, the Director, J-3, and the Director, J-6, on IO policy and strategy development.

(3) (U) Coordinate with the Director, J-7, for the incorporation of IO into operations plans and planning processes.

d. (U) The Director, J-6, will:

(1) (U) Coordinate with the Director, J-2, and the Director, J-3, to assist in IA policy and strategy development, validation of defensive capability requirements and programs for IA, the JWCA process, budget reviews and assessments, and technology development.

(2) (U) Ensure IA is integrated into deliberate and crisis planning in a manner consistent with DOD ID policy, strategy development and ID interface into OSD's Critical Infrastructure Protection programs.

(3) (U) Coordinate with the Defense Information Systems Agency (DISA), National Security Agency (NSA), Services, and other USG agencies, as appropriate, on IA matters, to include policy development and validation of capability requirements and programs for IA.

(4) (U) Represent the CJCS in IA-related interagency working groups.

(5) (U) Coordinate with the Director, J-7, on joint IA training, education, and exercises.

e. (U) The Director, J-7, will:

(1) (U) Coordinate with the Services, combatant commanders, CSAs, and the Joint Staff to develop joint IO doctrine.

(2) (U) Coordinate individual and collective joint IO training to meet emerging joint doctrine principles. Refine IO doctrine through

joint training events and exercises including conditions that stress our forces and their information systems and capabilities in realistic scenarios. As appropriate, promulgate IO lessons learned in the Joint Universal Lessons Learned System (JULLS).

(3) (U) Ensure IO is incorporated into joint professional military education curriculums.

(4) (U) Update the Joint Operation Planning and Execution System (JOPES) to reflect the need for deliberate planning for IO.

(5) (U) Ensure IO is integrated into the Universal Joint Task List (UJTL).

(6) (U) Ensure capabilities to conduct IO are fully addressed in the deliberate plans during the plan review process.

(7) (U) Ensure IO is incorporated into joint exercises, and assess IO as part of the Chairman's Exercise Evaluation Program.

f. (U) The Chairman's Legal Counsel will:

(1) (U) Provide legal reviews as requested to support IO policy development and implementation of IO tactics, techniques, or rules of engagement.

(2) (U) Provide legal review of plans prior to approval for execution as required.

g. (U) The Chairman's Special Assistant for Public Affairs (PA) will:

(1) (U) Provide PA review of Joint Staff/OSD plans and policies to ensure PA and information operations efforts are complementary.

(2) (U) Ensure PA activities support the Chairman's IO objectives consistent with the DOD Principles of Information, applicable policy, and statutory limitations.

h. (U) The combatant commanders will:

(1) (U) Conduct peacetime information activities in support of national goals and objectives as directed by the Joint Strategic Capabilities Plan (JSCP).

(2) (U) Integrate IO into deliberate and crisis plans in accordance with appropriate policy and doctrine (references j and l) to accomplish their UCP assigned missions.

(3) (U) Develop a process within the CINC and JTF staffs that effectively integrates the various capabilities and activities to conduct IO.

(4) (U) Incorporate IO tactics, techniques, and procedures into exercises, modeling and simulation, and training events using the Joint Mission Essential Task List (JMETL) process.

(5) (U) Identify IO capability requirements and submit appropriate mission need statements (MNSs) to the CJCS for validation using the guidance contained in reference m.

(6) (U) Develop, maintain, and prioritize IO requirements.

(7) (U) Develop IO intelligence requirements in support of all pertinent operational plans.

(8) (U) Identify IO training and exercise modeling and simulation requirements to the Joint Warfighting Center (JWFC).

(9) (U) Collaborate with JWAC and JC2WC in modeling and simulations (M&S) development.

(10) (U) Identify IO education requirements to Director, J-7.

(11) (U) Capture IO lessons learned from joint after-action reviews and submit to the Director, J-7, as part of the joint after-action report.

(12) (U) Plan and coordinate FDOs using IO along with traditional FDOs such as shows of force and military exercises.

(13) (U) Joint force legal counsel will provide legal review of IO plans prior to approval consistent with DOD Law of War Program (reference e).

i. (U) The Chiefs and USCINCSOC will:

(1) (U) Conduct research, development, testing, and evaluation of and procure capabilities that meet validated Service and joint IO requirements.

(2) (U) Maintain liaison with Services, Defense agencies, and other appropriate agencies to minimize duplication of effort in capabilities' development.

(3) (U) Identify intelligence requirements applicable to capabilities being developed or fielded. Coordinate with Defense Intelligence Agency (DIA) and the Joint Staff to ensure these requirements are communicated to the Intelligence Community.

(4) (U) Incorporate IO into Service school curriculums and into appropriate training and education activities. Both offensive and defensive aspects of IO must be addressed.

(S) (U) Organize, train, and equip forces to conduct IO. Ensure Service IO activities effectively support the CINCs through the appropriate Service component commanders.

(6) (U) Exercise IO (including fielded capabilities) in an environment representative of wartime and other realistic scenarios.

(7) (U) Coordinate with DIA, NSA, other intelligence agencies, and DISA to ensure development and population of data bases supporting collaborative planning, analysis, and execution of IO.

(8) (U) As required, develop Service IO policy, doctrine, and tactics that complement emerging joint doctrine.

(b)(1)

(10) (U) The Military Service Counterintelligence (CI) and Criminal Investigative Organizations will:

(a) (U) Assist the DIA in providing threat evaluation of foreign intelligence organizations and identifying CI requirements.

(b) (U) Investigate incidents of computer crime in support of CND.

(c) (U) Collect and disseminate threat information, and conduct other CI activities in support of IO.

j. (U) The Commander, JTF-CND, will:

(1) (U) Determine when system(s) are under strategic attack, assess impact to military operations and capabilities, and notify NCA and user community.

(2) (U) Coordinate and direct appropriate DDD actions to stop attack, contain damage, restore functionality, and provide feedback to user community.

(3) (U) Develop contingency plans, tactics, techniques, and procedures to defend DOD computer networks; support CINC deliberate planning for same.

(4) (U) Assess effectiveness of defensive actions and maintain current assessment of operational impact on DDD.

(S) (U) Coordinate as required with National Communications Systems (NCS), National Infrastructure Protection Center (NIPC), DOD Law Enforcement Agencies (LEAs), DOD CI organizations, civilian law enforcement, other Interagency partners, private sector, and allies.

(6) (U) Monitor status of DDD computer networks.

(7) (U) Monitor Computer Emergency Response Team (CERT) Alerts, Warnings and Advisories, and provide input to and monitor Indications and Warning (I&W) reporting.

(8) (U) Participate in joint training exercises to conduct CND.

(9) (U) Coordinate with Defense-wide Information Assurance Program (DIAP) and Critical Asset Assurance Program (CAAP) authorities to ensure JTF compliance with wider IA policy and initiatives.

(10) (U) Provide Intelligence Community with Priority Intelligence Requirements for collection and I & W requirements for potential attacks against DOD computers and networks.

(11) (U) Subject to authority, direction, and control of the Secretary of Defense, provide information to and receive direction from the Chairman of the Joint Chiefs of Staff and provide liaison as required to the OSD staff and Joint Chiefs of Staff.

k. (U) The Director, National Security Agency (DIRNSA), will:

(b)(1)

(S) (U) Provide INFOSEC technology, products, and services to help protect against hostile CNA efforts.

(6) (U) Conduct vulnerability and threat analysis to support information protection and the defense and protection of US and friendly information systems.

(7) (U) Coordinate with Defense Intelligence Agency (DIA), Services, other intelligence agencies, and Defense Information Systems Agency (DISA) to ensure development and population of databases supporting collaborative planning, analysis, and execution of IO.

(8) (U) As Executive Agent, ensure Joint Communications Monitoring Agency (JCMA) support is provided for defensive IO efforts.

l. (U) The Director, DIA, will:

(1) (U) Manage Defense Intelligence Community production to support the full range of DOD IO.

(2) (U) Oversee DOD intelligence requirements and serve as the Defense Intelligence Community focal point for the development, management, and maintenance of support databases and information systems that facilitate the timely dissemination of all-source, finished intelligence in support of DOD IO.

(3) (U) As DOD human intelligence (HUMINT) manager, provide oversight, guidance, and direction to the Defense HUMINT Service, consistent with DOD IO.

(4) (U) Assist combatant commanders with the development of command intelligence architecture planning programs that fully integrate IO support requirements.

(5) (U) Provide precise and timely intelligence for IO target selection and analysis and assessment of results on target to the combatant commands and Joint Staff.

(6) (U) As requested, provide direct intelligence assistance to the combatant commanders in the planning and execution of ID across the range of military operations.

(7) (U) Develop standards for Global Command and Control System (GCCS)-compliant IO support databases and coordinate with the Services, NSA, and DISA to ensure subsequent database population.

(8) (U) Provide indications and warning of foreign ID (including CNA), with the assistance of DISA and other government and non-government agencies.

(b)(1)

(10) (U) Provide intelligence certification of all weapons acquisition programs for IO in accordance with CJCSI 3170.01.

m. (U) The Director, DISA, will:

(1) (U) Ensure effective measures are taken to protect the defense information infrastructure (DII) from hostile network attack.

(2) (U) Coordinate with DIA, NSA, and the Services to ensure population of databases supporting collaborative planning, analysis, and execution of IA.

(3) (U) In coordination with other government and non-government agencies, assist DIA in providing indications and warning of CNA against US information systems and infrastructure.

(4) (U) Maintain liaison with the Office of the Secretary of Defense (OSD), the Joint Staff, the combatant commanders, the Services, CSAs, and other USG agencies to minimize the duplication of effort in capabilities' development for IA and to ensure interoperability and mutually reinforcing security policies, procedures, and systems.

n. (U) The Commander, Joint Command and Control Warfare Center (JC2WC), in coordination with USCINCACOM will:

(1) (U) As requested, provide support in accordance with reference l.

(2) (U) In concert with the Services, assist in the integration of IO opposition force activities (Red Teaming) conducted in the joint exercise arena.

o. (U) The Commander, Joint Warfighting Center (JWFC), will:

(1) (U) Collect, identify, and ensure combatant command and Service IO requirements are satisfied by present and future modeling and simulation systems.

(2) (U) Through the Modeling and Simulation Support Activity:

(a) (U) Ensure modeling and simulation efforts are coordinated to eliminate duplication of effort and help focus on the development of systems that fulfill combatant command and Service

IO training and exercise requirements. Ensure verification, validation, and accreditation (VV&A) of these models and simulations.

b. (U) Coordinate with Defense Modeling and Simulation Office to stay apprised of other agency modeling and simulation efforts that could support combatant command and Service requirements.

(3) (U) Coordinate and assist the Joint Staff, Services, and combatant commanders in developing joint IO doctrine.

p. (U) Commander, Joint COMSEC Monitoring Activity (JCMA), will:

(1) (U) Provide COMSEC monitoring and analysis support.

(2) (U) Provide a joint COMSEC monitoring and analysis team to provide direct, deployable joint COMSEC monitoring support.

(3) (U) Conduct crypto and/or telecommunications system monitoring efforts.

(4) (U) Provide timely, tailored reporting to supported commanders, to include near-real-time reporting of inadvertent disclosure of friendly critical information identified in the OPSEC process.

q. (U) The Commander, Joint Spectrum Center (JSC), will:

(1) (U) Provide locational and technical characteristics about friendly force C2 systems.

(2) (U) Provide assistance in development of the joint restricted frequency list (JRFL) for deconfliction purposes.

(3) (U) Provide assistance in the resolution of operational interference and jamming incidents.

(4) (U) Provide data about foreign C4 frequency and location data.

(5) (U) Provide unclassified C4 area studies about regional C4 infrastructure, to include physical and cultural characteristics, overview of telecommunications systems, and electromagnetic

frequencies registered for use within the geographic boundaries of each country in the region.

r. (U) Commander, Joint Warfare Analysis Center, will provide analysis of engineering and scientific and integrates operational analysis with intelligence data.

s. (U) The Director, Information Operations Technology Center (IDTC), will:

(b)(1)

t. (U) All DDD elements will adopt a risk management approach to protect their information, information systems, and information-based processes based on potential vulnerability to adversary ID.

ENCLDSURE C

REFERENCES

a. DOD Directive S-3600.1, 9 December 1996, "Information Dperations (U)"

b. DDD Instruction S-3600.2, 6 August 1998, "Information Dperations Securlty Classification Guidance (U)"

c. DOD Directive 3321.1, 26 July 1984, "Overt Peacetime PSYDP Programs"

d. DOD Instruction 5000.2, 23 February 1991, "Defense Acquisition Management Policies and Procedures"

e. DOD Directive S100.77, 10 July 1979, "DoD Law of War Program"

f. DOD Directive S160.S4, "Critical Asset Assurance Program"

g. CJCSI 3110.02, 01 January 199S, "Supplemental Instruction to JSCP FY1996: Intelligence Planning Objective Guidance and Tasks"

h. CJCSI 3110.0S, 01 July 1997, "Joint Psychological Dperations"

i. CJCSI 3110.1S, 12 May 199S, "Supplemental Instruction to JSCP FY1996: Special Technical Operations (STO)"

j. CJCSI 3122.03, 1 June 1996, "Joint Operational Planning and Execution System," Volume II

k. CJCSI 3170.01, 13 June 1997, "Requirements Generation System"

l. CJCSI 3210.03, 22 November 1996, "Joint Electronic Warfare Policy"

m. CJCSI 3211.01A, 15 June 1994, "Joint Military Deception"

n. CJCSI 3213.01, 1 December 1997, "Joint Operations Security"

o. CJCSI 5118.01, 15 September 1994, "Charter for the Joint Command and Control Warfare Center"

p. CJCSI 6510.01, 22 August 1997, "Defensive Information Operations Implementation"

q. Joint Pub 1-02, "Department of Defense Dictionary of Military and Associated Terms"

r. Joint Pub 2-01.02, "Joint Doctrine, Tactics, Techniques, and Procedures for Counterintelligence Support to Operations"

s. Joint Pub 3-13, 9 October 1998, "Joint Doctrine for Information Operations"

t. Joint Pub 3-13.1, 7 February 1996, "Joint Doctrine for Command and Control Warfare (C2W)"

u. Joint Pub 3-51, 30 June 1991, "Electronic Warfare in Joint Military Operations"

v. Joint Pub 3-53, 10 July, 1996, "Doctrine for Joint Psychological Operations"

w. Joint Pub 3-54, 24 January 1997, "Joint Doctrine for Operations Security"

x. Joint Pub 3-58, 31 May 1996, "Joint Doctrine for Military Deception"

y. Joint Pub 3-61, 14 May 1997, "Doctrine for Public Affairs in Joint Operations"

GLOSSARY

Definitions. Definitions are from reference a unless listed below; the following definitions are approved for future inclusion into Joint Publication 1-02, "Department of Defense Dictionary of Military and Associated Terms." The following terminology applies:

1. Computer network attack (CNA). Operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.

2. Computer network defense (CND). Measures taken to protect and defend information, computers, and networks from disruption, denial, degradation, or destruction.

3. Computer network exploitation (CNE). Intelligence collection operations that obtain information resident in files of threat automated information systems (AIS) and gain information about potential vulnerabilities, or access critical information resident within foreign AIS that could be used to the benefit of friendly operations.

4. Counter-propaganda. Efforts to negate, neutralize, or diminish the effects of or gain advantages from foreign propaganda efforts.

5. Information. Facts, data, or instructions in any medium or form.

6. Information Assurance (IA). IO that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

7. Information-based-processes. Processes that collect, analyze, and disseminate information using any medium or form. These processes may be stand-alone processes or sub-processes which, taken together, comprise a larger system or systems of processes.

8. Information environment. The aggregate of individuals, organizations, or systems that collect, process, or disseminate information; also included is the information itself.

9. Information operations (IO). Actions taken to affect adversary information and information systems, while defending one's own information and information systems. (NOTE: As the joint warfighting community gains experience in the employment of IO, the current definition of IO may be too narrow. As IO evolve, the definition of IO in DOD Directive 3600.1, "Information Operations" should be reviewed to ensure full joint warfighting effectiveness.)

10. Information systems. The entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information.

11. Information superiority. The capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same.

12. Information warfare (IW). Information Operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries.

13. Special information operations (SIO). IO that by their sensitive nature, due to their potential effect or impact, security requirements, or risk to the national security of the US, require a special review and approval process.